



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,460	06/30/2003	Tzong-Fen Fuh	50325-0799	1623
29989 7590 02/25/2008 HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110				
EXAMINER WHIPPLE, BRIAN P				
ART UNIT 2152		PAPER NUMBER		
MAIL DATE 02/25/2008		DELIVERY MODE PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/611,460

Applicant(s)

FUH ET AL.

Examiner

Brian P. Whipple

Art Unit

2152

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 December 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SG/US)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-30 are pending in this application and presented for examination.

Response to Arguments

2. Applicant's arguments, see pages 15-16, filed 12/13/07, with respect to the 35 U.S.C. 112, second paragraph rejections have been fully considered and are persuasive. The 35 U.S.C. 112, second paragraph rejections have been withdrawn.
3. Applicant's arguments, see pages 17-18, filed 12/13/07, with respect to 35 U.S.C. 103(c) have been fully considered and are persuasive. The corresponding 35 U.S.C. 103(a) rejections, based partially upon the invalid *Sitaraman* reference, have been withdrawn.
4. Applicant's remaining arguments are directed to amended subject matter and are properly addressed in the prior art rejections below.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a

person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-9, 13-19, 22-23, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baize, U.S. Patent No. 6,317,838 B1, in view of Sadovsky, U.S. Patent No. 5,689,638, and further in view of Welcher, Peter J. ; Reflexive Access Lists; 5/5/99; Chesapeake NETCRAFTSMEN (Hereafter referred to as Welcher).

7. As to claim 1, Baize discloses a system for controlling access of a client to a network resource (Abstract, ln. 1-3), the system comprising:

a network resource that is communicatively coupled to a network (Fig. 1; Col. 5, ln. 13-22);

a network firewall routing device that is communicatively coupled to the network and that is logically interposed between the client and the network resource (Fig. 1; Abstract, ln. 1-3; Col. 6, ln. 3-9), wherein the network firewall routing device comprises:

a firewall that protects the network resource by means for selectively blocking messages initiated by client and directed to the network resource (Abstract; Col. 6, ln. 3-9 and 13-26);

an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information (Fig. 1, Security Server SS; Abstract, ln. 5-11);

means for creating and storing client authorization information at the network firewall routing device, based in part on the user profile information, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource (Col. 6, ln. 58 – Col. 7, ln. 14; Col. 8, ln. 4-6);

means for receiving a request from the client to communicate with the network resource (Col. 4, ln. 38-42);

means for determining whether the client is authorized to communicate with the network resource based on the authorization information (Col. 4, ln. 43-48); and

means for creating a new user profile information, based on the user profile information, that includes the current IP address (Abstract; Col. 5, ln. 28-31; Col. 6, ln. 13-26).

Baize may be interpreted as disclosing means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information (Col. 6, ln. 33-42; Col. 7, ln. 15-18), wherein the means for reconfiguring the network firewall routing device further comprises: means for determining a current IP address of the client (Col. 6, ln. 13-26). The network firewall routing device

must be configured to permit clients to access network resources when authorized in order to function according to its intended purpose.

For the sake of argument, the examiner will assume Baize is silent on means for reconfiguring the network device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information.

However, Sadovsky discloses means for reconfiguring the network device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information (Col. 9, ln. 66 – Col. 10, ln. 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by reconfiguring a network device to permit a client to access network resources when authorized as taught by Sadovsky in order to avoid the need to request authentication data from a user (Sadovsky: Col. 9, ln. 66 – Col. 10, ln. 6).

Baize and Sadovsky may be interpreted as disclosing
the firewall comprises:

an external interface and an internal interface; and

an Output Access Control List at the internal interface and an Input Access

Control List at the external interface; and

means for adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the internal interface.

It is extremely well known in the art that a firewall consists of an internal and external interface, as is the existence of Input and Output ACLs on firewalls, and additionally, the fact that such ACLs are not permanent, burned-in definitions of access rules. One of the known benefits of a firewall is the ability to dynamically add, modify, and remove rules relating to access.

However, for the purposes of argument, the examiner will assume Baize and Sadovsky are silent on the aforementioned limitations and provide evidence of such in a separate prior art document, namely Welcher.

Welcher discloses
the firewall comprises:

an external interface (Page 2, Figure, item B) and an internal interface (Page 2, Figure, item A); and

an Output Access Control List at the internal interface and an Input Access Control List at the external interface (Page 2, ¶ 5); and

means for adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the

internal interface (Page 1, ¶ 6 – Page 2, ¶ 2; Page 2, ¶ 5; Welcher's created temporary access lists relating to users may be interpreted as user profile information; additionally, Baize discloses user profile information as discussed above).

8. As to claim 2, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for creating and storing client authorization information comprises means in the network firewall routing device for caching client authorization information for each client that communicates with the network firewall routing device (Sadovsky: Col. 9, ln. 66 – Col. 10, ln. 6).

9. As to claims 3-4, the claims are rejected for the same reasons as claim 2 above.

10. As to claim 5, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for determining whether the client is authorized to communicate with the network resource comprises means for matching information in the request identifying the client to information in means for filtering in the network routing device and to the authorization information stored in the network firewall routing device (Baize: Col. 4, ln. 38-48).

11. As to claim 6, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device (Baize: Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65); and means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 14).

12. As to claim 7, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a means for filtering in the network routing device (Baize: Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65); means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 14); and

means for matching user identifying information received from the client to a profile associated with the user that is stored in the authentication server if the source IP address fails to match the authorization information stored in the network firewall routing device (Baize: Col. 6, ln. 62 – Col. 7, ln. 18).

13. As to claim 8, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device (Baize: Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65);

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 14); and

means for matching user identifying information received from the client to a profile associated with the user that is stored in a database server and is retrieved from the database server by the authentication server, if the source IP address fails to match the authorization information stored in the network firewall routing device (Baize: Fig. 1, Data Base DBS and Security Server SS; Col. 5, ln. 28-31; Col. 6, ln. 62 – Col. 7, ln. 18).

14. As to claims 13 and 19, the claims are rejected for the same reasons as claims 4 and 8 above.

15. As to claim 9, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for determining whether the client is authorized to communicate with the network resource comprises: means for matching client identifying information in the request to information in a filtering mechanism of the network routing device (Baize: Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65);

means for matching the client identifying information to the authorization information stored in the network firewall routing device, if a match is found using the filtering mechanism (Baize: Col. 6, ln. 66 – Col. 7, ln. 14); and

means used, only when the client identifying information fails to match the authorization information stored in the network firewall routing device, for: creating and storing new authorization information in the network firewall routing device that is uniquely associated with the client (Baize: Col. 6, ln. 58 – Col. 7, ln. 14; Col. 8, ln. 4-6);

requesting login information from the client (Baize: Col. 6, ln. 62-65);

authenticating the login information by communicating with the authentication server (Baize: Col. 6, ln. 62 – Col. 7, ln. 2); and

updating the new authorization information based on information received from the authentication server (Baize: Col. 6, ln. 66 – Col. 7, ln. 14).

16. As to claim 14, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 1, including means for reconfiguring the network firewall routing device comprises means for creating and storing one or more commands to the network firewall routing device which, when executed by the network firewall routing device, result in modifying one or more routing interfaces of the network firewall routing device to permit communication between the client and the network resource (Baize: Col. 6, ln. 62 – Col. 7, ln. 18).

17. As to claim 15, the claim is rejected for the same reasons as claim 1 above.

18. As to claim 16, the claim is rejected for the same reasons as claim 4 above.

19. As to claim 17, the claim is rejected for the same reasons as claim 6 above.

20. As to claim 18, the claim is rejected for the same reasons as claim 8 above.

21. As to claim 22, Baize discloses a system for authentication comprising: a network resource connected to a network (Fig. 1; Col. 5, ln. 13-22);

a client capable of sending a request to communicate with the network resource (Col. 4, ln. 38-42);

a network firewall routing device that is logically interposed between the client and the network resource and that permits the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on client authorization information stored in the network firewall routing device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource (Col. 6, ln. 58 – Col. 7, ln. 14; Col. 8, ln. 4-6);

a database server that stores a plurality of user profiles, each user profile uniquely associated with one of a plurality of users that can use the client to send requests to communicate with the network resource (Col. 5, ln. 28-31);

an authentication server that is logically interposed between the network firewall routing device and the database server, and that is capable of communicating with the database server and retrieving from the database server a user profile (Fig. 1, Data Base DBS and Security Server SS; Col. 5, ln. 28-31; Col. 6, ln. 62 – Col. 7, ln. 18).

The limitation from the previous amendment filed on 7/12/07 of “reconfigured to permit” is rejected for the same reasons as claim 1 above, per the previous Office action mailed on 9/11/07.

The limitations added by the amendment filed on 12/13/07 are rejected for the same reasons as claim 1 above.

22. As to claim 23, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 22, including the network resource comprises a target server capable of servicing a request sent under at least one of HyperText Transfer Protocol; File Transfer Protocol (Baize: Col. 6, ln. 33-36); and Internet Control Message Protocol.

23. As to claim 25, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 22, including the network firewall routing device comprises: one or more processors (Baize: Fig. 2; Col. 6, ln. 13-26; it is inherent that a firewall executing access decisions contains one or more processors); and

a storage medium carrying one or more sequences of one or more instructions including instructions which, when executed by the one or more processors (Baize: Fig. 2; Col. 6, ln. 13-26; Col. 7, ln. 3-14; it is inherent that a firewall storing an operational profile has a storage medium), cause the one or more processors to perform the steps of:

creating and storing the client authorization information at the network firewall routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 18);

receiving the request from the client to communicate with the network resource (Baize: Col. 6, ln. 58-61);

determining whether the client is authorized to communicate with the network resource based on the client authorization information (Baize: Col. 6, ln. 62 – Col. 7, ln. 18);
and

permitting the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the client authorization information (Baize: Col. 6, ln. 62 – Col. 7, ln. 18).

24. As to claim 26, the claim is rejected for the same reasons as claim 14 above.

25. As to claim 27, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 25, including determining whether the client is authorized to communicate with the network resource comprises the steps of: determining whether client identifying information in the request matches information in a filtering mechanism of the network firewall routing device (Baize: Col. 6, ln. 58-65);

if a match is found using the filtering mechanism, determining whether the client identifying information matches the client authorization information stored in the network firewall routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 18); and

only when the client identifying information fails to match the client authorization information stored in the network firewall routing device (Baize: Col. 6, ln. 66 – Col. 7, ln. 18), then:

creating and storing new client authorization information in the network firewall routing device that is uniquely associated with the client (Baize: Col. 6, ln. 66 – Col. 7, ln. 18);

requesting login information from the client (Baize: Col. 6, ln. 62-65);

authenticating the login information by communicating with the authentication server (Baize: Col. 6, ln. 66 – Col. 7, ln. 18); and

updating the new client authorization information based on information received from the authentication server (Baize: Col. 6, ln. 66 – Col. 7, ln. 18).

26. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baize, Sadovsky, and Welcher as applied to claim 1 above, in view of Coss et al. (Coss), U.S. Patent No. 6,170,012 B1.

27. As to claim 12, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 9, but are silent on means for creating and storing an inactivity timer for each authentication cache, wherein the inactivity timer expires when no communications are directed from the client to the network resource through the network firewall routing device during a pre-determined period of time, and means for removing the updated authentication information when the inactivity timer expires.

However, Coss discloses means for creating and storing an inactivity timer for each authentication cache, wherein the inactivity timer expires when no communications are directed from the client to the network resource through the network firewall routing device during a pre-determined period of time, and means for removing the updated authentication information when the inactivity timer expires (Col. 4, ln. 45-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize, Sadovsky, and Welcher by utilizing an inactivity timer to remove cache entries as taught by Coss in order to free up space in a cache and in order to improve security by requiring an inactive client to re-authenticate.

28. Claims 10-11, 20-21, 24, and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baize, Sadovsky, and Welcher as applied to claims 9, 15, 22, and 27 above, in view of Klassen, U.S. Patent No. 6,216,121 B1.

29. As to claim 10, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 9, including means for the network firewall routing device requesting login information from the client to solicit a username and a user password (Baize: Col. 6, ln. 62-65) and means for authenticating the login information comprises means for determining, from a profile associated with a user of the client stored in the authentication server, whether the username and password are valid (Baize: Col. 6, ln. 66 – Col. 7, ln. 2), but are silent on sending a Hypertext Markup language login form to the client.

However, Klassen discloses sending a Hypertext Markup language login form to the client (Fig. 5; Col. 5, ln. 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize, Sadovsky, and Welcher by using a Hypertext Markup language login form as taught by Klassen in order to make use of a standard means for a client to login to a system and in order to authenticate the identify of the client.

30. As to claim 11, the claim is rejected for the same reasons as claims 8 and 10 above.

Art Unit: 2152

31. As to claim 21, Baize, Sadovsky, and Welcher disclose the invention substantially as in parent claim 15, but are silent on the client in a computer system executing a Web browser.

However, Klassen discloses the client in a computer system executing a Web browser (Fig. 5; Col. 5, ln. 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize, Sadovsky, and Welcher by using a Web browser as taught by Klassen in order to make use of a standard means for a client to communicate with the Internet.

32. As to claim 24, the claim is rejected for the same reasons as claim 21 above.

33. As to claims 20 and 28-29, the claims are rejected for the same reasons as claim 11 above.

34. As to claim 30, the claim is rejected for the same reasons as claim 10 above.

Conclusion

35. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Whipple whose telephone number is (571)270-1244. The examiner can normally be reached on Mon-Fri (8:30 AM to 5:00 PM EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571) 272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2152

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brian P. Whipple
/B. P. W./
Examiner, Art Unit 2152
2/18/08

/Bunjob Jaroenchonwanit/
Supervisory Patent Examiner, Art Unit 2152